DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON DC 20310-1001

REPLY TO
ATTENTION OF
DAMI-CD (380-67)

26 Jan 05

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Changes to Procedures re: Submission of Personnel Security Investigations (PSIs); and the Use of the Joint Personnel Adjudication System (JPAS)

1. This memorandum supersedes all prior Army guidance on the submission of PSI's and the use of JPAS. The guidance contained herein is applicable to all Army activities as well as other DoD activities that submit PSI on Army personnel.

2. Effective 14 Februrary 2005, JPAS is the Army's system of record to determine clearance eligibility and current command access level. This change is necessary and desirable in order to provide a single location to input, maintain and retrieve eligibility and access data on all DoD personnel. The procedures for implementation and use of JPAS within the Army are contained in enclosure (1). No later than 11 April 05, all Security Management Offices will be established and all owning/servicing relationships for Army personnel will be established. Also effective 11 April 05, except as outlined in enclosure (1), all communication with the Army Central Clearance Facility (CCF) will be via JPAS. No later than 9 May 05, all Army personnel will have their Non-Disclosure Agreement (NDA) and access information entered into JPAS.

3. Effective immediately, all Army PSI's formerly submitted to DSS via the Electronic Personnel Security Questionnaire (EPSQ), will be submitted to a separate P.O. Box at the Office of Personnel Management (OPM). This change eliminates the electronic transmission of PSI's to Defense Security Service (DSS) and aligns the transmission of all PSI's to OPM (separated by type). This change will provide faster investigation open times and the ability for OPM to directly contact submitting offices to resolve discrepancies. Enclosure (2) contains specific instructions for all submissions.

4. Points of contact are Ms. Julia Swan, (703) 695-2629/DSN 329-2629, e-mail: julia.swan@hqda.army.mil, or Mr. Greg Torres, (703) 695-2360/DSN 329-2360, e-mail: gregory.torres@hqda.army.mil. All inquiries should be addressed through command channels.

Thomas A. Gandy

Encls

Thomas A. Gandy
Director, Counterintelligence, Human
Intelligence, Disclosure and Security

DISTRIBUTION
Commander, Eighth Army, ATTN: Unit #15236 (EAGB/ACofS, G2)
Commander, U.S. Army Europe and Seventh Army, ATTN: AEAGB-SAD-S
Commander, U.S. Army Forces Command, ATTN: AFIN-SD,
Commander, U.S. Army Criminal Investigation Command, ATTN: CICG-SC,
Commander, Chief, National Guard Bureau, ATTN: NGB-SDS (Ms. Gravely),
Commander, Military Traffic Management Command, ATTN: Director G1/G4 Command Security
Commander, U.S. Army Corps of Engineers, Office of Security & Law
Enforcement, ATTN: CECS-OI
Commander, U.S. Army Intelligence and Security Command, ATTN: IASE-IS,
Commander, U.S. Army Medical Command, ATTN: MCOP-O-SI,
Commander, U.S. Army Pacific Command, Office of the DCSINT,
ATTN: APIN-SC (Mr. Dennis Quigley)
Commander, U.S. Army Training and Doctrine Command, ATTN: ATIN-SE,
Commander, U.S. Army Materiel Command, ATTN: AMXMI-SCM,
Commander, U.S. Army Test and Evaluation Command, ATTN: CSTE-OP-SSI
Commander, U.S. Army Military District of Washington, ATTN: ANOP-S,
Commander, U.S. Army South, ATTN: SOIN-SD
Commander, U.S. Army Special Operations Command, ODCS, G-2,
Commander, U.S. Army Test and Evaluation Command, ATTN: CSTE-OP-TST,
Director, Installation Management Agency
ATTN: SFIM-OP (Mr. Don Stout)
U.S. Army Space and Missile Defense Command, ATTN: SMDC-IN-S
U.S. Army Records Management and Declassification Agency
US Army Network Enterprise Technology Command/9th Army Signal Command
DoD Homeland Security Office, ATTN: Security Manager
HQDA, Office of the Administrative Assistant to the Secretary of the Army, ATTN: Chief, Personnel & Physical Security Division
Army National Guard Readiness Center, ATTN: NGB-ARO-I

JPAS System of Record Procedures

1. Effective 14 Feb 05, Commands with access to the Joint Personnel Adjudication System (JPAS) are to use the Joint Clearance and Access Verification System (JCAVS), a subsystem of JPAS, to perform the functions listed below. Commands/units that do not yet have JPAS access, will obtain that access and comply with the requirements listed below no later than 11 Apr 05.

a. Establish JPAS accounts: CCF will be the Army Account Manager for Army MACOMs, Reserve Command HQ, Reserve Support Commands, and the National Guard Bureau, to include the 50 State and US Territory National Guard HQ. Each MACOM will appoint an Account Manager. MACOM JPAS Account Managers will be given level 2 and/or level 4 accounts as appropriate. MACOM JPAS Account Managers will in turn create appropriate accounts for their subordinate units and subordinate Security Managers (SMs)/Special Security Offices (SSOs). Account Managers will also ensure that all SMs/SSOs have the appropriate level of access based on their duties, training and scope of responsibility. When creating Security Management Offices (SMOs) within JPAS, ensure that the following information is filled in as described below on the Security Management Office Maintenance Screen. All fields with asterisks will also be filled in.

(1) SMO Name: Enter the Command Name and the physical location. For the location portion, use the same location construct as outlined in #2 below. (e.g. Army HQ, G-2, Washington, DC or Army Materiel Command, Fort Belvoir, VA)

(2) SMO Location: Option 1 - Base, State or Country; Option 2 - City, State or Country (e.g. Fort Polk, LA or Washington, DC or Stuttgart, Germany)

(3) e-mail: Primary SM/SSO POC Name, Phone, email; Alternate SM/SSO POC Name, Phone, email. (e.g. Joe Soldier, (123) 555-1234, joe.soldier@us.army.mil; Jane Civilian, (123) 555-4321, Jane.civilian@us.army.mil)

This will cause the SMO fields on the Person Summary page to look like this:
Army HQ, G-2, Washington, DC, John Soldier, (123) 555-1234, joe.soldier@us.army.mil; Jane Civilian, (123) 555-4321, Jane.civilian@us.army.mil This will make it easier for SMs/SSOs to track down and contact other security offices, especially when a member needs to be out-processed at their losing command prior to being in-processed at their new organization. An owning relationship can be established with only one SCI and one non-SCI SMO. This information can only be updated by an account manager and should be updated whenever critical information changes.

b. Training: Account Managers will ensure that all personnel with access to JPAS have received the appropriate live or online training prior to being granted system access. The approved training module can be found at the JPAS web site as a link on the left hand side titled "training". The web site is: https://jpas.osd.mil/. Once that link is selected, choose the link for Joint Integrated Training Application (JITA). Complete the "Account Management" and/or "Security Management" training modules (as appropriate) by selecting the appropriate link; choosing the "describe it" link; followed by going through all of the other internal links. After receiving the training, take the test for each module in order to obtain certificates. There is also an excellent desk-top reference that can be found by clicking on the JCAVS Desktop Resource (August 2004) link, that is further down on the JPAS Training Web Page. This resource will answer most frequently asked questions.

c. Establish Owning/Servicing relationship/PSM Net: Each SM/SSO will create a relationship with each individual that they are responsible for. Every individual must be owned by someone in order for JPAS notifications (adjudications, suspensions, etc) to be transmitted to owners and servicing offices. To determine what type of relationship should exist, use the following guidelines.

(1) SSOs will take an "owning" relationship of all Sensitive Compartmented Information (SCI) cleared personnel that are in their SCI billets by becoming their SCI SMOs.

(2) SSOs will take "servicing" relationship of all SCI personnel that they are providing support to when the individual's SCI billet is held by another command/organization.

(3) Security Managers will take an "owning" relationship of all personnel within their command/unit by becoming their non-SCI SMOs. This will provide local Security Managers/Commands/Units with visibility of the status of all of their personnel. It will also cause initial questions regarding clearance issues to be directed to the local Security Manager.

(4) Security Managers will take a "servicing" relationship of all personnel that they do not "own" but for whom they provide supporting services to. (This may include Consolidated Security Offices that provide final transmission of Personnel Security Investigation (PSI) forms and/or maintaining official security records) This will also ensure that servicing security offices can have oversight for all supported personnel and units. These consolidated security offices, in coordination with the owning office, will determine which personnel security functions will be performed by each office. Two important guiding principles should be adhered to. First, duplication of effort will be avoided. Second, functions retained by an owning office should be based on that offices ability to effectively execute those functions. For example: Owning offices that service less than 25 personnel, should consider having most of their functions performed by the consolidated office. Owning offices that do not have trained "0080-Security Specialists" to perform personnel security functions should also consider having their functions performed by their consolidated security office. Where none of the above conditions apply, it seems appropriate that consolidated security offices would provide support and assistance to the owning organizations.

(5) Contractor Security Officers have access to JPAS. They will own their personnel and enter the individual into JPAS. Defense Industrial Security Conversion Office (DISCO) will enter the GENSER adjudication information. The Army Central Clearance Facility (CCF) will enter the SCI adjudication Information. The contractor will enter the GENSER access information. The Army Contractor Support Element (CSE) will enter the SCI access information. Army SSOs and SMs will establish servicing relationships with their contractor personnel. CSE may request administrative assistance for SCI indoctrinations and may request that the local SSO enter the Indoctrination information into JPAS. SCI Indoctrination oaths and Non-Disclosure Statements (NDS) will be sent back to CSE.

d. Use JPAS to Communication with CCF: Communications with CCF to request the following services will now be accomplished via the JPAS link on the Person Summary screen.

(1) DA Form 5247: The Request to Research, Recertify/Upgrade Eligibilty (RRU) function in JPAS will replace the DA Form 5247. A statement of verification of citizenship, the document used for verification, and dates of continuous federal service will continue to be provided with each RRU submission. The RRU function will not be used for the following:

a. Name changes (refer to JPAS website FAQ);

b. Downgrading of clearances;

c. Requests for adjudication of closed PSI (Except when the PSI has been closed for more than 4 months);

d. Requests for clearance conversions/transfer when the required level is reflected in JPAS.

(2) DA Form 5248-R: Unfavorable Information Reports.

a. The DA Form 5248-R (Report of Unfavorable Information for Security Determination) will be eliminated. The unfavorable information reporting requirement will be accomplished via the JPAS Report Incident Link on the Person Summary Screen.

b. Enclosures or other supporting documentation previously submitted in conjunction with a 5248-R will be forwarded to CCF either by e-mail (INCIDENTREPORT@CCF1.ftmeade.army.mil) or when email is not available, by FAX (COMM: 301-677-2703, DSN: 622).

c. Security Managers will be the only persons authorized to submit incident reports. Owning and Servicing security offices will coordinate prior to submission.

d. Incident reports will contain the following information:

1. Basis of Report - offense/allegation;

2. Action Taken;

a. Commander's Recommendation;

b. Any supporting documentation being forwarded to CCF;

c. Name, grade, title and contact telephone number of the submitting security manager, annotated at the end of the summary.

(3) Requests for Interim SCI Access: This function now will also be accomplished via JPAS (Person Summary Screen). Documentation supporting a request for interim SCI will be sent to CCF by e-mail INTERIMSCI@CCF1.ftmeade.army.mil or when email is not available, by FAX (COMM: 301-677-2706, DSN: 622.

(4) Green Mailers: Effective with the implementation of JPAS, CCF green mailers will be eliminated. Information currently provided via green mailers that is not routinely reflected in JPAS will be disseminated in the "Notifications Link, Message to CAF". **REMINDER**: CCF will not be able to communicate with SMs/SSOs that do not have an owning or servicing relationship of the subject in question.

e. Verify current clearance level eligibility: Current eligibility for classified material access authorization will now be done by sighting the "eligibility" field on the Person Summary screen. Listed adjudications are valid for all DoD users, regardless of which agency made the adjudication (e.g. there is no need to request re-adjudication for an Army member solely because the listed adjudication was done by Navy. The information in this field only indicates the highest appropriate adjudication decision made. This field DOES NOT equate to the individuals current access level. The level of information that an individual currently has access to will be entered into JPAS by SMs/SSOs using the "Indoctrinate" link. In order to grant an individual access to classified information they must have: Current eligibility and a signed a Non-Disclosure Agreement (NDA). These are the guidelines for granting access based on JPAS information.

(1) SCI Access may be granted when the Person Summary Screen shows:

a. DCID 6/4 eligibility within the past 5 years; a SSBI within the past 5 years; and no break in service of more than 24 months; or

b. The Person Summary Screen shows DCID 6/4 eligibility, a completed SSBI beyond five years and a submitted SSBI-PR. SSOs must review the PSI to ensure that no-significant derogatory information exists in order to indoctrinate without CCF review. There must also be no break in federal service (as defined in AR 380-67, 1-306.1) of more than 24 months.

(2) Top Secret access may be granted when the Person Summary Screen shows Top Secret eligibility and the subject meets the same investigative/ derogatory/break in federal service requirements outlined in para 1.e(1)a or b above.

(3) Secret access may be granted when the Person Summary Screen shows:

a. Secret eligibility determination within the past 10 years; a PSI within the past 10 years; and no break in federal service of more than 24 months (If subject is a Federal Civilian employee in a Non-Critical/Sensitive position, ensure that the subject meets the requirements for Federal Civilian suitability as proscribed by your local personnel office. This may require a ANACI.); or

b. Secret eligibility determination; an outdated PSI that met the scope of investigation for Secret eligibility at the time of the previous adjudication; no break in federal service of more than 24 months; and a newly submitted periodic reinvestigation. Again, the SM must review the PSI and local files to ensure that no-significant derogatory information exists in order to determine eligibility without CCF review. (Federal Civilian suitability determinations outlined in para a. above also apply.)

(4) In cases outlined above where the only issue is a break in federal service, submitting a new PSI will negate the disqualifying condition.

f. Verify current authorized access level: The access levels listed in JPAS under Non-SCI Access and SCI Access are entered by the subject's SMs and SSOs. This information will be used to grant access at both the individual's parent organization, as well as visited organizations within the DoD. Internal access rosters for DoD personnel that are not derived from JPAS are no longer authorized. The transmission of written "visit requests" is no longer required and will only be used when required by the visiting organization. Army Command/Units with access to an individual's clearance/access information via JPAS will not require that clearance information be transmitted to them via other means.

g. In-Processing: When in-processing personnel, SMs/SSOs will establish the appropriate relationship with their supported personnel as described in para 1.c. above. In addition, SMs/SSOs may take a servicing relationship of personnel that are inbound until they are released from their prior organization, at which time the relationship may be adjusted.

h. Indoctrinate: When granting personnel access, SMs/SSOs will ensure that the appropriate NDA or NDS date is recorded in the system. Once the system contains the appropriate NDA and/or NDS date, a new NDA/NDS will not be executed. The access grant date will also be entered for each level of access granted (e.g. Secret, Top Secret, SI, TK, etc).

i. Interim Security Clearance Determinations: Currently, JPAS users may only input interim clearances/accesses if the subject meets criteria as outlined in AR 380-67. A modification will be added that will allow entering interim clearances/access once the "EPSQ Sent" date is filled in by the SM, vs. having to wait until the investigation actually shows as open. In the mean time, interim access may continue to be granted after following all of the current requirements as outlined in AR 380-67, to include submission of the PSI to Office of Personnel Management (OPM). Placing the PSI in the U.S. Mail or other courier service is sufficient to meet the requirement of "submitted". However, Security Managers must remember to enter the clearance/access once the investigation shows open in JPAS. We will modify this interim requirement once the functionality in JPAS is modified.

j. Input Personnel Security Investigation Sent Date: For all personnel who have had PSIs submitted, but whose investigation is not yet completed, the EPSQ date must be filled in. This will allow you to not only issue interim clearances, but it will also allow Army to track the length of time it takes to open cases from the time of submission. It will also assist JPAS in notifying the submitter if a submitted case does not open after a certain amount of time (this notification will be available in JPAS at a later date).

k. Determine Status of Requested Personnel Security Investigations: Security Managers/SSO's will periodically check the "Person Summary" screen of JPAS to ensure that pending investigations have progressed appropriately (e.g. opened/scheduled, closed). This is especially critical within the first 30 days after submission of an investigation to ensure receipt and action by OPM. Issues related to the status of open or not yet opened investigations will be directed to OPM. Issues related to closed investigations pending adjudication, will be addressed to Army CCF using the RRU function, after an appropriate amount of time (currently 6 months) following case closure.

l. Unofficial Foreign Travel: SM/SSOs will ensure that unofficial foreign travel is reported by employees with clearances and is entered into JPAS via the "Unofficial Foreign Travel" link.

2. For military or federal civilian personnel not listed in JPAS, use the Test Problem Report (TPR) function to report a "data" problem. The "Problem Title" should be "Record Not Found in JPAS". Include the following information in the "Detailed Description" block: Subject's full name, SSN, DOB and affiliation (e.g. Active Army, Reserve, Civilian, etc). This action may take up to 72 hours. There will be a modification made to JPAS in the future that will speed up this process. The current

web address for TPR's is: https://jpas.osd.mil/hai_jpas/login3.asp. The TPR link/site will soon change and will be added to the new JPAS web-site.

3. It is important to remember that OPM is the organization that conducts investigation for DOD. The Army CCF is the organization that reviews the cases and makes adjudication determinations. Please direct your questions to the appropriate organizations after you check the status in JPAS. We expect that we will have a liaison at OPM sometime in mid-FY05.

4. Please use the chain of command for JPAS related questions.

MAIL PSI REQUESTS DIRECT TO OPM

1. All Army PSI requests will be submitted in paper to OPM, until the Electronic Questionnaire for Investigation Processing (E-QIP) is deployed in DoD (est. Summer CY 2005).

a. All Army activities must have an OPM assigned SON before submitting PSI's to OPM.

b. The Standard Form (SF) 86, "Questionnaire for National Security Positions," is the traditional form used to request PSI's from OPM. The SF 86 may be downloaded from OPM's web site at: www.opm.gov. At top bar click on "Site Index", select "F" from alphabetical listing, select "Forms" from topics, select "Standard Forms (SF)" from electronic forms, then select "SF 86" to print a copy.

c. Commands may complete the SF 86 and mail it, with the required fingerprint card, directly to OPM. The SF 86 incorporates the required releases and Agency Use information. (A hand written submission is not the preferred choice.)

d. DoD commands also have the option of using a printed EPSQ in lieu of the SF 86 (This is the preferred method). If you use a printed EPSQ, you must ensure the EPSQ is validated and all errors are corrected. You must also attach the necessary release forms and Agency Use Form along with the required fingerprint cards to complete the request package. The Agency Use information is a mandatory part of all OPM PSI requests. OPM will not process an EPSQ request without a completed AGENCY USE FORM. (A copy of the Agency Use Form and Instructions is attached.)

e. The following OPAC-ALC codes will be used as applicable:

(1) DoD-Army – investigations for newly assigned civilian employees.

(2) DA-GPSI – investigations for Army Military personnel and civilian periodic reinvestigations.

(3) DSS-Ind – investigations for contractor (industry personnel submitted via SF 85P.

(4) Army CYS – child care cases (unless a different code has been established by local arrangement with OPM.

f. Mail all completely assembled PSI request packages (including Release Forms and Finger Print cards "where appropriate") to OPM as follows:

For military submission (excluding accessions personnel), mail PSI packages to:
US Office of Personnel Management
Federal Investigations Processing Center
BOX 49
1137 Branchton Road
Boyers, PA 16018

For military accessions & civilians, mail PSI packages to:
US Office of Personnel Management
Federal Investigations Processing Center
BOX 618
1137 Branchton Road
Boyers, PA 16018

g. You are required to maintain a copy of all submitted PSI request packages until final adjudication is completed.

h. In addition to mail time, OPM takes up to 7 days to in-process and open a request. Check the SII link on the Joint Clearance and Access Verification System (JCAVS) periodically to ensure OPM receives and acts on your request. If after mail time plus 10 business days your request still has not opened at OPM, contact OPM to determine if a resubmittal is necessary.

2. Effective immediately, submitters will no longer cancel investigations that have been submitted when the subject separates from service (civilian or military). This action will be handled centrally at the DoD level (it will be triggered when the subject is no longer owned in JPAS for over 30 days). If however, JPAS reflects that the individual is still owned by a Security Manager/SSO, even though the military and/or civilian personnel system indicates a separation from service, the owning Security Manager/SSO will be contacted by DoD for verification prior to case cancellation. If the subject is not currently owned by a Security Manager/SSO, DoD will simply notify the last known owner. Security Managers/SSOs will still continue to out-process separated personnel in the JPAS system.

Procedures to Clear Backlog of Army Non-Actionable Cases

1. Approximately 25,000 request for PSIs forwarded electronically to DSS cannot be opened; mostly due to missing fingerprint cards or missing signed release forms. Commands that submitted electronically to DSS are directed to check the Joint Personnel Adjudication System (JPAS) to determine if the investigation is pending. If the investigation is pending, there is no further action necessary. If it is not pending, check the DSS EPSQ Receipt System on the DSS web site at www.dss.mil. to determine if required Finger Print or Release Forms have been received. If one or both of these documents has not been received by DSS, the case cannot be opened. If there is a receipt for the investigation in the EPSQ receipt system, but the investigation is not open (according to JPAS), take the following steps.

a. If the request is less than 90 days old (based on the date the subject signed the EPSQ/Release forms), mail the missing information to DSS immediately. Allow normal mail time plus 5 business days processing time for mailed information to reach DSS and be entered into the EPSQ receipt system. If the missing information does not reach DSS in time for them to match them to the EPSQ and transport them to OPM (Boyers, PA), before the 120 day mark from date of signature, the case will be rejected. Use this address to mail missing releases/FP cards to DSS.

National Agency Records Processing Group
Defense Security Service
601 10th Street, Suite 325
Fort George, G. Meade MD 20755-5134

If the release form is the only missing item, you may still fax a copy to DSS in accordance with the instruction on the DSS web-site at: http://www.dss.mil/epsq/faxreleasecvr.htm.

b. If the request is over 90 days old (or if the missing Release Forms/FP Cards will not reach DSS/OPM before the 120 day point), submit a new investigation to OPM via the appropriate address in the enclosure. Include all required forms (e.g. agency use form, SF 86, Release Form, Finger Print cards (not required for PRs), etc.)

c. In the case of personnel that are currently deployed and not available to provide new/current signatures and forms, follow the procedures outlined in HQDA G-2 message DTG 121628Z Feb 03, that states in part:

Compliance with periodic Reinvestigation (PR) requirements will continue, except as follows:

-Submissions for deployed Enduring Freedom personnel are not required until 90 days after return from deployment.

-If "Stop Loss" is enacted, personnel affected are exempt from submission of PRs.

2. Questions concerning these procedures may be addressed to Julia Swan, (703) 695-2629.